

National Aeronautics and Space Administration



NASA Consolidated Active Directory Overview (August 20, 2012)

Office of the Chief Information Officer

***NASA IT Vision:** The NASA IT
Organization is the **very best**
in government*



Les Chafin
Infrastructure Engineering
HPES



Introduction



- Les Chafin; Infrastructure Engineering Manager
 - » HPES NASA ACES
- Responsible for:
 - » Active Directory, Exchange Engineering Team



Agenda



- NASA Consolidated Active Directory (NCAD)
- Active Directory Domain
- Disaster Recovery
- OU Structure
- Active Directory Management Suite
 - » ADMS – Directory and Resource Administrator (DRA)
 - » ADMS – Group Policy Administrator (GPA)
- Security Monitoring of Active Directory (SMAD)



- NCAD Enterprise Program
 - » Active Directory Domain
 - » Active Directory Management Suite (ADMS)
 - » Security Monitoring of Active Directory (SMAD)



Active Directory Domain



- ndc.nasa.gov
- Single Forest; Single Domain
- 2008 R2 Forest and Domain Functional Level
- Centralized Management
- Domain Controllers Located at Every Center
 - » Redundant DC's – At least two at every center
 - » NASA E-Mail System
 - » ASA Data Center Networks
- NASA IP Address Management (IPAM) DNS – Primary
 - » Underscore Zones Delegated



Continuity of Operations



- AD Fully Redundant
 - » Every DC has a Writable Copy of AD Database
- NCAD Core Systems Backed Up
- Core Active Directory Roles Fully Transferable
- Disaster Recovery
 - » Fully Exercised Every 3 Years



OU Structure



- Active Directory Account Management Provided by NASA Identity, Credential, and Access Management (ICAM) Team
- Typical Accounts OU Configuration
- Domain.nasa.gov
 - » Accounts
 - *cc1*
 - *cc2*
 - *cc3*

Note: cc = Two Letter NASA Center Code



OU Structure



- Typical NASA Center Level OU Configuration
- *cc*
 - » *cc-org1*
 - *cc-orgGroups*
 - *cc-orgSrv*
 - *cc-orgWS*
 - » *cc-org2*
 - *cc-org2Groups*
 - *cc-org2Srv*
 - *cc-org2WS*

Note: cc = Two Letter NASA Center Code



Active Directory Management Suite (ADMS)



- Provides NASA Systems Administrators with the Ability to Manage AD Objects
- No Native AD Rights Required by NASA Systems Administrators
- Provides Audit Trail and Change Tracking
- Components:
 - » NetIQ Directory and Resource Administrator (DRA)
 - » NetIQ Group Policy Administrator (GPA)



- Role Based Administration
- Proxies Rights to Manage AD Objects
- Core Support Infrastructure
 - » Primary DRA Server
 - » Agency Accessible Web Consoles
- DRA Server Located at Each Center
 - » Web Console
 - » Scripting Capability
- Smart Card Access



DRA Roles



- Agency Roles
 - » Agency Help Desk
 - » Account Administrators
- Center OU Roles
 - » System Administrator
 - » Account Administrator 1
 - » Computer Support Specialist 1 and 2
 - » Help Desk
 - » Group Membership Management
- Center Sub OU Roles
 - » System Administrator
 - » Account Administrator 1
 - » Computer Support Specialist 1 and 2
 - » Group Membership Management



DRA OU Roles



Type of Privileged User Roles	Password Reset	Add/ Delete from Groups	Create/Delete Computer Accounts	Create/ Delete Groups
Help Desk (ND-GG-ADMS-cc-HD)	x			
Account Administrator 1 (ND-GG-ADMS-cc-Acct1)		X (User Accounts)		
Computer Support Specialist 1 (ND-GG-ADMS-cc-CS1)			x	
Computer Support Specialist 2 (ND-GG-ADMS-cc-CS2)		x (Computer accounts)	x	
System Administrator (OU Admin) (ND-GG-ADMS-cc-SA)	x	x (in OU and GPO groups)	x	x
Group Membership Role (Controls membership in named security groups)		X (User and Computer in Named Groups only)		



- Role Based Administration
- Manage and Track Changes to Group Policy Objects
 - » Changes Reviewed and Approved before Export to AD
 - » Allows Roll Back to Previous Version
- GPO's Exported to Domain After Core Team Review
- Centralized Infrastructure



GPA Roles



- GPO Importer/Editor
 - » Center Level Role
 - » Edit or Import GPO's in the database
- GPO Approver
 - » Center Level Role
 - » Approves GPO Changes for Their Center
- GPO Export
 - » Role Held by Members of NASA Core AD Core Team
 - » Export Approved GPO's After Review



- Security Monitoring for Active Directory (SMAD)
 - » Provides Centralized Security Log Management
 - » Event Monitoring, Correlation, Alerting, and Response
 - » Security Reporting
- Designed to Monitor and Alert
 - » NASA Consolidated Active Directory (NCAD)
 - » Active Directory Management System (ADMS) environments
 - » Security Monitoring for Active Directory (SMAD) system self monitoring



SMAD Overview



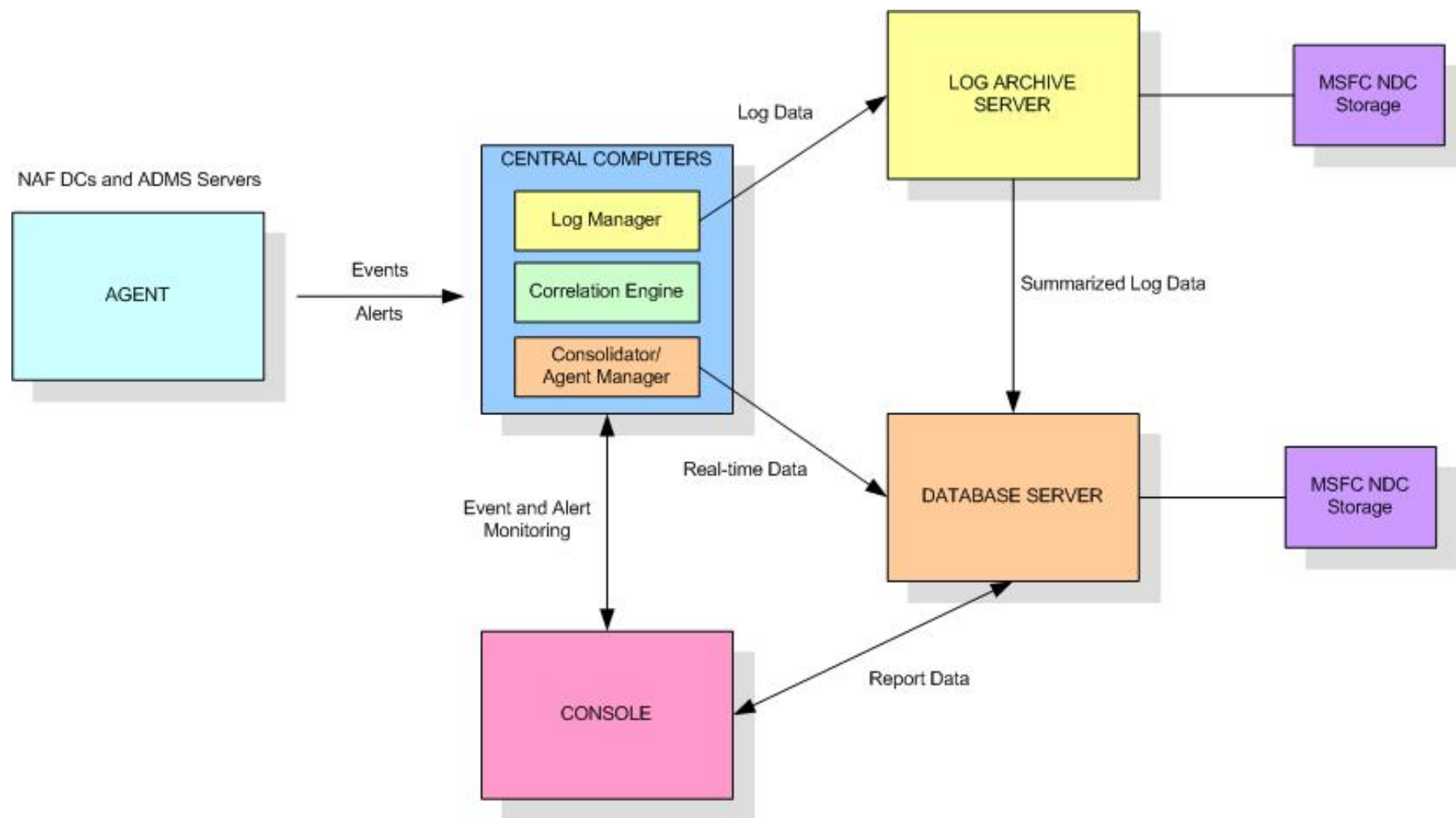
- Server Communicates via IPSEC Tunnel to Clients
 - » Uses AES Encryption for all Log Traffic
- All Data is Digitally Signed Before Stored
- SMAD Protections
 - » Limited Direct Access
 - » Self Monitoring
 - » Separation of Roles
 - » File Integrity Checking
 - » Process Checking
 - » Change Monitoring
 - » Privileged User Monitoring
- Investigations
 - » Incident Response
 - » Tracking for Support Groups Throughout Agency
 - » Additional Active Directory Team Internal Investigations
 - » SMAD Team Works with NCAD and Centers Incident Response Teams



SMAD Overview: Components



- SMAD Comprised of Three COTS Components
 - » NetIQ Security Manager (SM)
 - Real-time Monitoring of System Changes and User Activity
 - Detection of threats and intrusions
 - Security event management and correlation
 - Central log management
 - Incident response automation
 - » NetIQ Change Guardian for Active Directory (CGAD)
 - Monitors AD and provides alerting for unmanaged changes
 - Software module for SM
 - » NetIQ Change Guardian for Windows (CGW)
 - Monitors OS level, files and directories, file shares, registry and system processes and provides alerting
 - Software module for SM





SMAD Statistics



- SMAD Entered Production Status 8/12/08
- 6 SMAD Production Servers
- 92 SMAD Agents
- 361,677,155 Events per week (Week of July 23rd – 2012)
 - » AN Average of 51,668,165 Events/Day
 - » Approx. 5,000 Alerts/Day
 - Warnings, Errors, Critical Errors, Security Breaches, etc...
 - » PEAK 83 million Events/Day
- Security Log Archive Data
 - » 7+ TB of Compressed Forensic Data



Questions?





Backup Slides





NCAD Operations



- ACES Data Center Operations Monitoring Team
 - » 24x7
- NCAD Patch Support
 - » Windows Server Update Services (WSUS)
 - » Patch Monthly based on MS Patch Release Schedule
- Server Health Monitoring
 - » System Centers Operations Manager (SCOM)
- Centralized Anti-Virus Management
 - » Symantec Endpoint Manager
 - » Symantec Endpoint Client



ESD Helpdesk



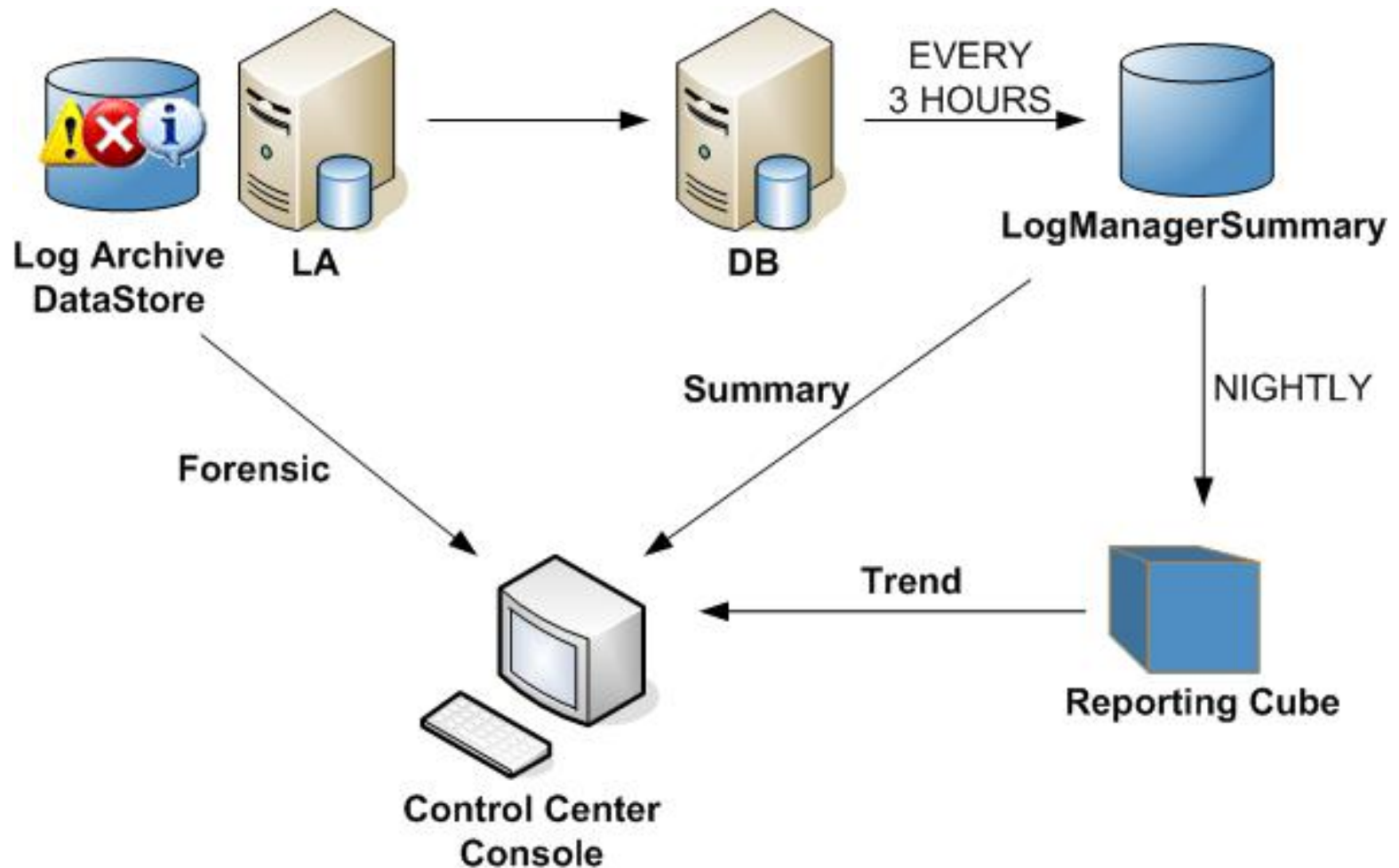
- 24x7 Support
- DRA Agency Helpdesk Role
- Account Unlock, Password Reset, Account Enable



SMAD : Purpose Cont.

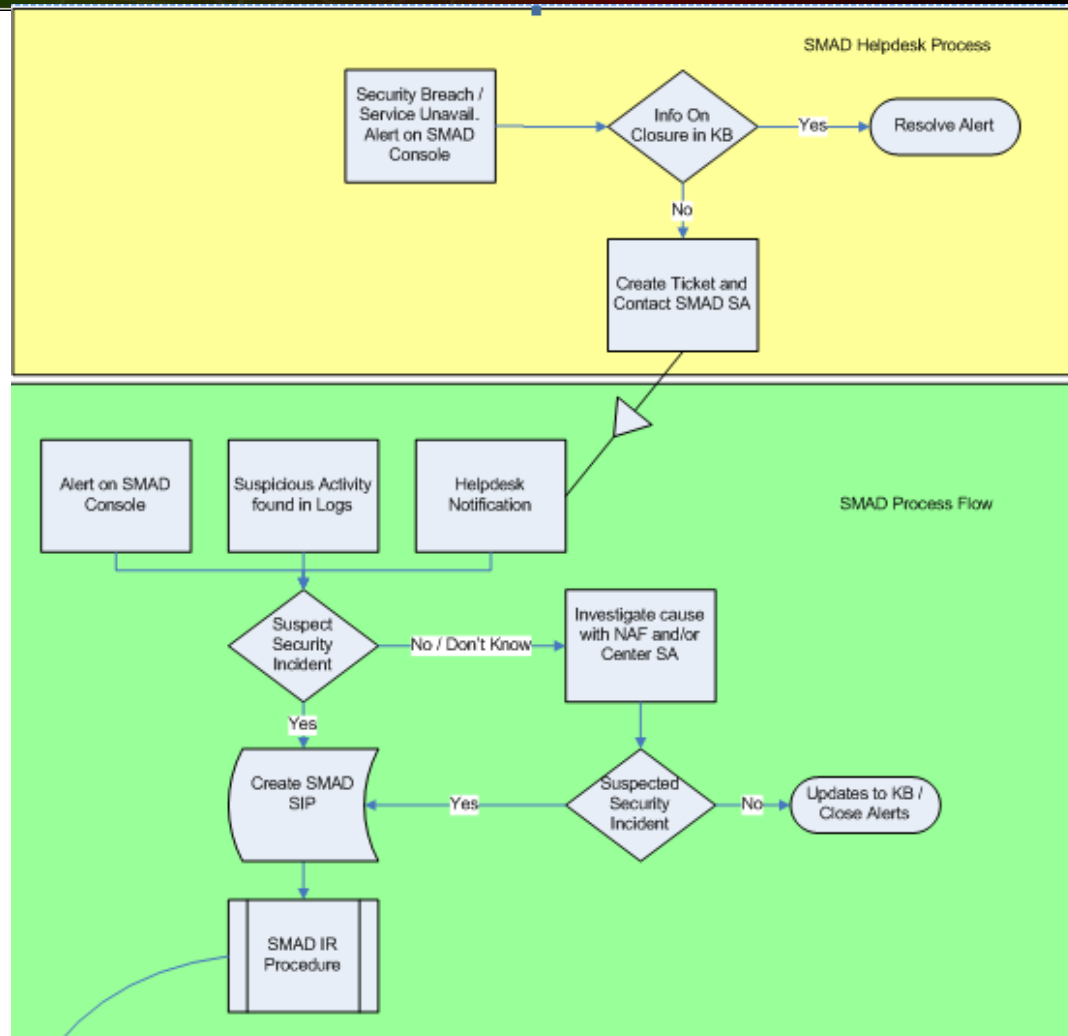


- SMAD helps meet requirements of FISMA and NIST Standards of security review, reporting, and remediation planning.
- Of particular mention for log management, SP 800-53—Guide for the Security Certification and Accreditation of Federal Information Systems
 - » Within SP 800-53 are multiple controls that recommend regular review and monitoring of audit logs, especially within the Audit & Accountability Controls set, and Access Controls set.
- SP 800-92
 - » Section 2.3.1 NIST accepts and recommends Federal Agencies to utilize systems that normalize and centralize logs for faster response to incidents and remediation.
 - » Section 2.3.2 NIST specifies that host-based intrusion detections (HIDS) products are particularly helpful in finding patterns that humans cannot easily see such as correlating entries from multiple logs that relate to a single incident. Specifies that log analysis should be proactive not reactive. To achieve this logs must be reviewed in real-time or near-real-time manner. Without sound processes the value of the logs is significantly reduced.

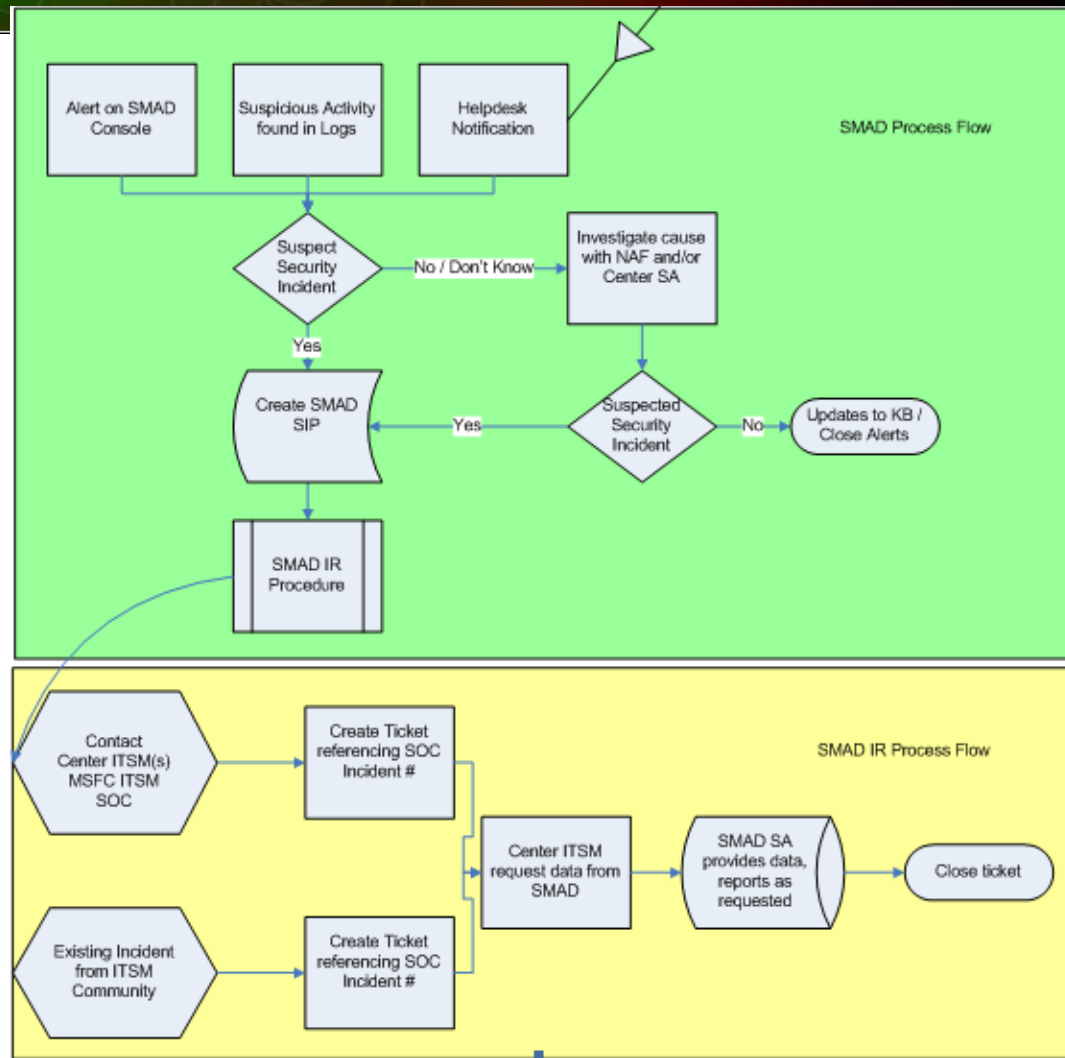


Alert Response Process

- Alert- Console and email
- KB Populated with known issues
- Unknown conditions escalated to SMAD SA and SMAD SE
- SMAD SA receives alerts or call from NISC
- Investigates and evaluates condition
- Creates starting SIP
- Initiates IR Procedure



- IR Process can be internally or externally initiated
- Ticket filed with NISC
- Incident opened at SOC
- MSFC and center ITSM(s) notified
- Data given to ITSM
- Incident Closed with SOC
- Ticket Closed
- Resolution Phase
 - KB Updated
 - Rules Updated
 - Other policy, procedure changes if needed





IR process



- SMAD SLA's
 - First 30 minutes following a notification of a new alert : Staff is responsible to acknowledge the alert and decide if the alert is a false positive or requires further investigation
 - First 1 hour following notification: SMAD Must assign a staff member to investigate the alert using NAF / ADMS Support Staff as needed
 - First 1 hour following classification of Alert as an incident:
 - Severity and classification of incident with SOC by US-Cert Standards
 - Center(s) involved in the incident. (Including MSFC ITSM and OCSO)
 - SOC must be notified and an incident number assigned
 - Within 14 days: Alert must be resolved, and all technical person(s) completed their remediation activities
 - SMAD SA or SE will create a SMAD Incident Package (SIP).
 - SIP contains reports, events, alerts and attachments for investigation
 - During this time the internal SMAD Resolution State will be set to Level 4 to keep the alerts active for 30 days.
 - Within 21 Days: Closeout procedure completed.
 - All Tickets closed / Incident Closed at SOC
 - Any restored logs to the log archive server have been detached and space allocated back to system
 - All items marked Level 4 are now marked resolved



Rules Overview



- Default Rule Set
 - Each module provides default rules
 - 3,600 rules were evaluated
 - Rules were enabled, disabled, customized
 - Rule re-writes for correctness and reduce false positives
- DRA and DMA Managed / Unmanaged Changes
 - Use of account tracked external to program
- Vulnerability Manager / Intrusion Manager
 - Scripts analyze registry
 - Services and Ports monitored
- CGAD / CGW
 - Managed / unmanaged changes
 - Track authorized / unauthorized changes



Rules Overview Cont.



- Antivirus Check points
- Self Monitoring
 - Heartbeat active
 - Self log checking
- Archive Rule for Security Logs
- Correlation / Collection Activity
 - Collects Suspicious Activity
 - OU Move
 - Logon Failure then Disabling Account
 - Multiple Failed logons
 - Logon Failure followed by Log Clearing
 - Successful Attacks
 - Failed logon followed by account creation
 - Account granted "act as operating system"
 - Failed admin logon followed by service account logon
 - Multiple account logout
 - User Enabled and Disabled in Rapid Succession



Rules Overview Cont.



- Customization
 - Standard Accounts Defined
 - High Profile Groups and Users Defined
- NetIQ Optimization
 - Rules updated to properly handle user & workstation accounts
- Custom Enhancement during Incident Resolution
 - Example: GPO Incident at a center
 - GPG Reports available needed better solution
 - New CGGP Solution only supports 32Bit DC's
 - Custom Alerts
 - SM Event Manager to detect event
 - CGW to detect changes within /sysvol/